**1. Введение**

**1.1 Актуальность разработки ПИБ**

Разработка политики информационной безопасности (ПИБ) становится жизненно важной для туристических компаний, поскольку они активно используют цифровые технологии для обработки персональных данных, бронирования туров и финансовых транзакций. Угрозы кибератак, утечек данных и мошенничества требуют серьезного внимания, поскольку нарушение безопасности может привести к утрате доверия клиентов, юридическим последствиям, штрафам и финансовым потерям. Взлом системы бронирования или утечка данных платежных систем могут вызвать серьезные репутационные и финансовые риски, а вредоносные программы и внутренние угрозы от недобросовестных сотрудников усугубляют ситуацию.

Несоблюдение политики безопасности может привести к значительным последствиям, включая утрату данных, юридические проблемы, нарушение законодательства и даже прекращение деятельности. Важнейшими мерами защиты являются внедрение комплексной системы защиты, обучение сотрудников, мониторинг угроз и соответствие нормативным требованиям, что позволит избежать угроз и обеспечит стабильную работу туристического бизнеса в цифровой эпохе.

**1.2 Цели и задачи ПИБ**

Целью данной политики является обеспечение защиты информации, хранящейся и обрабатываемой в информационно-вычислительных системах (ИВС) компании. Основные задачи:

* Обеспечение конфиденциальности, целостности и доступности данных.
* Минимизация рисков утечек и несанкционированного доступа.
* Разработка мер защиты от угроз, представленных в анализе рисков.
* Обучение сотрудников безопасному обращению с информацией.
* Контроль соблюдения политики безопасности.

**2. Объекты защиты**

**2.1 Структура организации**

Туристическая компания включает в себя:

* Центральный офис.
* Офисы продаж и филиалы.
* Веб-портал и мобильное приложение.
* Серверную инфраструктуру.
* Базы данных клиентов и партнеров.
* Каналы связи (VPN, корпоративная почта, мессенджеры).

**2.2 Периметр и внутренняя структура ИВС**

Периметр включает:

* Облачные сервисы, используемые для хранения данных.
* Внешние подключения (VPN, интернет-шлюзы).
* Серверы, базы данных, рабочие станции сотрудников.

**2.3 Субъекты информационных отношений**

* **Сотрудники компании** (менеджеры, бухгалтерия, IT-отдел).
* **Клиенты** (пользователи сайта, заказчики туров).
* **Партнеры** (гостиницы, авиакомпании, страховые компании).
* **Хакеры и злоумышленники** (потенциальные атакующие).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Описание атаки/угрозы** | **Ущерб** | **Вероятность** | **Риск** | **Мероприятия по обеспечению безопасности** |
| Фишинговая атака на сотрудников | 3 | 0,3 | 0,9 | Проведение тренингов по кибербезопасности, использование антивирусных решений, внедрение многофакторной аутентификации (MFA) |
| Взлом клиентских аккаунтов | 1 | 0,2 | 0,4 | Политика сложных паролей, мониторинг аномальной активности пользователей |
| DDoS-атака на веб-сайт | 2 | 0,3 | 0,6 | Использование средств защиты от DDoS (прокси-серверы (Cloudfare)) |
| Утечка персональных данных клиентов | 4 | 0,2 | 0,8 | Контроль доступа к данным, шифрование, аудит логов доступа |
| Кража ноутбука с конфиденциальными данными | 3 | 0,1 | 0,3 | Настройка удаленного блокирования устройств |
| Вредоносное ПО на рабочих станциях | 2 | 0,3 | 0,6 | Использование антивирусного ПО, регулярные обновления ПО, запрет установки стороннего ПО |
| Саботаж сотрудника (намеренное удаление данных) | 3 | 0,2 | 0,6 | Разграничение прав пользователей, резервное копирование данных, контроль действий сотрудников |
| Утрата доступа к облачным сервисам | 4 | 0,1 | 0,4 | Использование нескольких облачных провайдеров, локальное резервирование данных |
| Пожар в офисе | 5 | 0,1 | 0,5 | Системы пожаротушения |
| Отказ электропитания | 3 | 0,3 | 0,9 | Установка ИБП (источников бесперебойного питания), резервные генераторы |
| Сбой интернет-подключения | 2 | 0,4 | 0,8 | Использование нескольких интернет-провайдеров |
| Аппаратный сбой серверов | 4 | 0,2 | 0,8 | Горизонтальное масштабирование серверов |
| Программные ошибки (сбой системы бронирования) | 3 | 0,3 | 0,9 | Регулярное тестирование ПО, разработка процедур аварийного восстановления |
| **Итого** |  |  | **8,5** |  |

**1.1.5. Мероприятия по внедрению политики безопасности в туристической компании**

После разработки документации по информационной безопасности (ИБ) необходимо внедрить ее в повседневную работу компании. Основой таких мероприятий являются инструкции, содержащие подробное описание алгоритмов защиты данных и обеспечения стандартов ИБ, а также план мероприятий по обучению сотрудников и тестированию их знаний в области безопасности.

Можно выделить следующие основные направления мероприятий:

* **Управление персоналом**
* **Физическая защита инфраструктуры ИВС**
* **Поддержание работоспособности ИВС**
* **Реагирование на нарушения режима безопасности**
* **Планирование восстановительных работ**

**Управление персоналом**

Для каждого сотрудника, имеющего доступ к информационным ресурсам компании (системам бронирования, платежным системам, клиентским данным), должны быть установлены квалификационные требования по ИБ. В должностные инструкции необходимо включить разделы, касающиеся защиты информации.

Обучение сотрудников мерам ИБ включает в себя:

* Проведение вводных инструктажей при приеме на работу
* Регулярное обучение по распознаванию фишинговых атак, безопасному использованию ИТ-инфраструктуры
* Проведение тестов на знание политики ИБ

Также важно определить уровень доступа к различным системам в зависимости от должностных обязанностей сотрудника.

**Физическая защита инфраструктуры ИВС**

Физическая защита информационной инфраструктуры туристической компании включает в себя:

* Ограничение физического доступа к серверам, маршрутизаторам, рабочим компьютерам с критической информацией
* Использование видеонаблюдения и контроля доступа в серверные помещения
* Применение инженерных методов защиты от пожаров, затоплений и других угроз
* Обеспечение бесперебойного питания серверов и сетевого оборудования

**Поддержание работоспособности ИВС**

Для обеспечения бесперебойной работы информационной инфраструктуры компании необходимо:

* Регулярно обновлять программное обеспечение
* Обеспечивать резервное копирование данных (в том числе облачное хранение)
* Использовать антивирусное ПО и средства защиты от вредоносного ПО
* Ограничивать установку неавторизованных программ на рабочие станции сотрудников

Также стоит регламентировать работу с персональными данными клиентов, чтобы они хранились в зашифрованном виде и доступ к ним был строго ограничен.

**Реагирование на нарушения режима безопасности**

Компания должна разработать и утвердить план действий при выявлении инцидентов ИБ. Это может включать:

* Мониторинг активности пользователей и сетевого трафика
* Проведение расследований при утечках данных
* Блокировку учетных записей при подозрительной активности
* Наличие ответственного сотрудника или группы по реагированию на инциденты

Для мониторинга угроз можно использовать SIEM-системы или специализированные сервисы, анализирующие активность в корпоративной сети.

**Планирование восстановительных работ**

Для минимизации последствий возможных атак или сбоев необходимо заранее подготовить план восстановления, включающий:

* Регулярное тестирование резервных копий данных
* Создание резервных облачных хранилищ
* Разработку четкого алгоритма действий при потере доступа к основным системам (например, к системе бронирования)
* Определение ответственных лиц за восстановление работы ИВС

**Программно-технические меры обеспечения безопасности**

Основные механизмы защиты данных в туристической компании:

* **Идентификация и аутентификация пользователей** – использование надежных паролей и многофакторной аутентификации
* **Управление доступом** – ограничение прав пользователей в зависимости от их должностных обязанностей
* **Протоколирование и аудит** – ведение логов доступа и активности пользователей
* **Криптография** – шифрование персональных данных клиентов
* **Экранирование** – использование межсетевых экранов для защиты внутренней сети
* **Обеспечение высокой доступности** – создание отказоустойчивых серверов и резервных каналов связи

**Заключение**

Политика информационной безопасности туристической компании должна рассматриваться как комплекс мер, направленный на защиту информации клиентов и компании от внешних и внутренних угроз. Ее реализация требует участия всего персонала, применения современных технических решений и регулярного обновления процедур безопасности.